UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/771,967 | 01/30/2001 | Mehdi-Laurent Akkar | AKKAR | 2638 |

1444 7590 03/02/2011

Browdy and Neimark, PLLC
1625 K Street, N.W.
Suite 1100
Washington, DC 20006

| EXAMINER | |
|---|---|
| DAVIS, ZACHARY A | |
| ART UNIT | PAPER NUMBER |
| 2492 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 03/02/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/771,967 | AKKAR ET AL. | |
| | Examiner | Art Unit | |
| | Zachary A. Davis | 2492 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *15-19,22-24 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-19,22-24 and 27-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10 September 2010 has been entered.

2. By the above submission, Claims 19, 27-29, and 31-34 have been amended. No claims have been added or canceled. Claims 15-19, 22-24, and 27-34 are currently pending in the present application.

3. Applicant's request for suspension of action under 37 CFR 1.103(c) for a period of three months filed with the request for continued examination was proper and was granted. The period of suspension of action expired on 10 December 2010. It is noted that no supplemental reply was filed during such period of suspension of action.

### *Response to Arguments*

4. Applicant's arguments filed 10 September 2010 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 15-19, 22-24, and 27-34 under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783, Applicant has acknowledged the deficiencies noted in the declaration under 37 CFR 1.131 filed 28 October 2009 (detailed in the previous Office action mailed 10 March 2010). Applicant indicated that a supplemental declaration would be prepared and submitted with a supplemental response prior to the end of the period of suspension of action; however, no such supplemental reply or declaration has been received. Applicant has provided no other arguments with respect to this rejection.

Therefore, the Examiner maintains the rejection as set forth below.

***Claim Objections***

5. Claim 34 is objected to because of the following informalities:

Claim 34 recites the term "DPA" in line 3 of the claim. This abbreviation should be spelled out in full the first time it appears.

Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

6. The rejection of Claims 15-19, 22-24, and 27-34 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn. Although the amendments to the claims

have corrected some of the issues of indefiniteness, the amendments have also raised new issues of indefiniteness, as detailed below.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 34 recites the limitation "said plurality of operations comprising, for each operation of the first chain of operations, either said operation or the respective operation in the second chain of operations corresponding to said operation" in lines 21-24. The antecedent basis of the phrase "said operation". It is not clear to which operation "said operation" is intended to refer, because there are many different operations recited earlier in the claim. Because it is not clear which operation is referred to by "said operation", it is not explicitly clear which operation in the second chain would be considered to be the "respective operation" of "said operation". This renders the claim indefinite.

Claims 27 and 28 each recite "the step of storing at the microcircuit card". However, Claim 34 recites two steps of storing that both involve the microcircuit card. It appears that this may be intended to refer to the second step of storing that recites storing the second set of instructions, and such interpretation has been assumed for the purposes of interpreting the prior art. The claims also each recite "a respective one of the operations operation"; it is not clear to which operation this is intended to refer,

because it is not clear what the term "respective" is intended to refer to. That is, it is not clear what the one operation is described with respect to.

Claim 29 recites "a second set of instructions" in line 2. It is not clear whether this is intended to refer to the same second set of instructions as recited in Claim 34 or to a different set. For purposes of interpreting the prior art, it has been assumed that this is intended to read "the second set of instructions" or "said second set of instructions" or similar.

Claim 32 recites "the random selection of an operation" in line 4; however, the reference to selection of "an operation" is generally unclear since there are plural operations that are selected from either the first chain or the second chain of operations as recited in Claim 34. Note that the similar recitation in Claim 31 of "the random selection of the operations…" (see line 4 of that claim) does appear to clearly refer to the selection of plural operation as recited in Claim 34, in contrast to this limitation in Claim 32.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 34, Applicant admits as prior art a method including storing a first chain of operations that performs DES encryption, exchanging a message between a server entity and a microcircuit card, the server entity executing a first set of instructions applying a first chain of operations to the message to obtain a server result, the microcircuit card executing a second set of instructions applying a second chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly choosing a group of operations that include some combination of operations of first and second chains of operations in either a complemented or uncomplemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 22 and 31, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and a counter is updated (Kocher, column 9, lines 25-27; column 10, lines 13-column 11, line 26; column 11, lines 41-45).

In reference to Claims 23 and 32, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and intermediate responses are transmitted (see Kocher, column 2, lines 17-19), and Chow further discloses transmitting information with each executed operation (Chow, column 19, lines 22-34).

In reference to Claims 24 and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30; see also column 7, lines 21-29).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on (571) 272-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2492